REMARKS

This Amendment is submitted in reply to the Final Office Action dated April 27, 2010. Applicant respectfully requests reconsideration and further examination of the patent application pursuant to 37 C.F.R. § 1.113.

Summary of the Examiner's objections and rejections

Claims 8-13 stand objected to because they depend on cancelled claim 2.

Claims 1, 3-16, 18-25, and 27-30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Thomas (U.S. 2004/0039827) in view of Lev Ran (U.S. 2004/0255048).

Summary of Amendments

Applicant has amended claims 1, 8, 15, 21 and 25, and added new claim 31. The amendments to claims 1, 15, 21 and 25 were made to correct minor grammatical or punctuation errors. The amendment to claim 8 was made to correct an antecedent error. The support for the new claim 31 can for instance be found on found in paragraphs [0050], [0055], [0058], FIG. 4 and the original claim 1within the originally filed patent application. No new subject matter has been added.

Remarks regarding the objections

Claims 8-13 stand objected to because they depend on cancelled claim 2. Applicant has amended claim 8 to depend from claim 1 rather than the cancelled claim 2. Accordingly, Applicant respectfully requests the removal of this objection to claims 8-13.

Remarks regarding the §103(a) rejections

Applicant respectfully traverses the obviousness rejection of independent claim 1 in view Thomas, Lev Ran or any combination thereof. The independent claim 1 is as follows:

1. An Application Gateway Module suitable for use in a telecommunication system wherein a service network authenticates a user and authorizes the user for accessing a service offered by a service provider, the Application Gateway Module arranged for intercepting application messages between the user and the service and for identifying said user and said service, and including:

means for obtaining an authorization decision on whether the user is allowed to access the service;

the Application Gateway Module comprising:

means for assigning a service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;

means for configuring a first finite-state machine with a number of statuses intended to identify specific events in service delivery, the first finite state machine configured to control service progression

means for initiating a specific instance of the first finite-state machine, said specific instance being identified by the assigned service session identifier; and

means for activating service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier.

The closest prior art Thomas discloses in paragraphs [0064]-[0067] an intermediary server and the Examiner interprets this entity as reading-on the claimed Application Gateway Module. Thomas also discloses on paragraph [0259] an LSP intercepting calls, this LSP being part of a Microsoft OS such as Windows for securing communications to or from sockets. In addition, Thomas discloses on [0260] the LSP being part of the intermediary server. The Examiner also interprets this LSP as being part of the claimed Application Gateway Module. However, Thomas does not disclose where the LSP identifies the user and the service from the intercepted messages. Instead, LSP is intended to communicate different applications with Windows sockets and, as such, there is no disclosure where the LSP may identify a user accessing a service in a service network, simply because this is not a task for the LSP service. Thus, the interpretation made by the Examiner that the intermediary server with the LSP reads-on the claimed Application Gateway Module, which is arranged for intercepting application messages between the user and the service and for identifying said user and said service, is thus wrong.

In addition, Thomas discloses on [0073]-[0075] an authentication procedure carried out when the user first tries to login in the system, and when this authentication

is successful, the user is given a session identifier to be presented to access the various resources in the private network through the intermediary server. However, even if Thomas discloses a user authentication, these paragraphs fail to read-on the claimed means for obtaining an authorization decision on whether the user is allowed to access the service, since authentication and authorization are well known to be different techniques.

Furthermore, Thomas discloses on paragraph [0075] providing a session identifier to the requestor as a result of a successful authentication, this session identifier used in subsequent requests to the intermediary server as long as the session is active. Subsequent requests to the intermediary server may correspond to a same or to different services and, generally speaking, is related to the session established between the authenticated user and the intermediary server. As commented above, Thomas discloses on [0073]-[0075] "...the user is given a session identifier to be presented to access the various resources in the private network..." However, the claim 1 recites "assigning a service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user", that is, in claim 1 there is one service session identifier for each service delivery so that, where more than one service is delivered within a session, corresponding more than one service session identifiers are assigned. Consequently, the "session identifier used in subsequent requests to the intermediary server as long as the session is active" disclosed on paragraph [0075] of Thomas, even if similarly worded, does not anticipate the "service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user" recited in the pending claim 1.

Thomas also discloses on paragraph [0286] a state machine. In Thomas's disclosure, "the state machine is based on characteristics of the Windsock API and/or communication protocol API can handle the port mapped data". Apart from this paragraph being editorially confusing, this disclosure does not read-on "configuring a first finite-state machine with a number of statuses intended to identify specific events in

service delivery, the first finite-state machine configured to control service progression". Of course, any conventional state machine comprises a number of statuses, but it is the intention and function of the statuses and transitions between them which are relevant factors when prosecuting this patent application. In this respect, Thomas fails to disclose statuses intended to identify specific events in service delivery, because APIs are mere descriptions of how communications between layers are carried out, rather than service progression. Moreover, Thomas's paragraphs [0286]-[0287] deal with the selection of loopback addresses and ports involved in the LSP interception (already commented above) and this has nothing to do with the service progression of a service authorized for a user. Consequently, the specific state machine recited in claim 1 is different from the specific state machine disclosed in Thomas, which is at least a non-enabling disclosure.

Still with reference to Thomas's paragraph [0286], and in the light of paragraph [0069] the Examiner contends this disclosure teaches the claimed feature "initiating a specific instance of the first finite-state machine, said specific instance being identified by the assigned service session identifier". As already commented above, Thomas's paragraph [0286] merely discloses "the state machine is based on characteristics of the Windsock API and/or communication protocol API can handle the port mapped data" whereas Thomas's paragraph [0069] discloses the intermediary server including a cookie manager. This cookie manager manages cookies previously received from a remote server and stored until being delivered to the remote server at appropriate times. These cookies are said to be set by a remote server and used for session, state or identification purposes. That is, Thomas discloses on [0069] cookies set by the remote server, submitted from the remote server to the intermediary server (which the Examiner has constructed as the claimed Application Gateway module), stored at the intermediary server, and returned from the intermediary server to the remote server at appropriate times. This teaching does not suggest an "Application Gateway Module having means for initiating a specific instance of the first finite-state machine, said specific instance being identified by the assigned service session identifier" as recited in

claim 1, and by no means can be similarly interpreted even if isolated words like 'state' and 'session' appear in Thomas's paragraph [0069].

In this regard, Thomas's paragraph [0069] does not disclose the Application Gateway Module (intermediary server in the interpretation of the Examiner) having means for initiating a specific instance of the first finite-state machine cited on Thomas's paragraph [0286], so that there is no hint to combine cookies received from the remote server with "the state machine is based on characteristics of the Windsock API and/or communication protocol API can handle the port mapped data". Consequently, there is no disclosure or suggestion in view of Thomas's paragraphs [0069] or [0286] of identifying such (undisclosed) specific instance of the state machine by the assigned service session identifier. Therefore, one can unambiguously conclude that Thomas's paragraph [0069] cannot be naturally combined with paragraph [0286] and, even if combined, the paragraphs [0069] and [0286] fail to disclose the claimed "Application Gateway Module having means for initiating a specific instance of the first finite-state machine, said specific instance being identified by the assigned service session identifier". Moreover, combining the cookies received from a remote server, as disclosed in Thomas's paragraph [0069], with the state machine based on characteristics of the Winsock API, as disclosed in Thomas's paragraph [0286], does not make any technical sense for any person skilled in the art that uses cookies as identifiers and follows API's for communication between different applications or application layers.

Further, the Examiner refers to the secondary reference Lev Ran to find a citation of "activating service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier", which the Examiner recognizes is not disclosed in the closest prior art Thomas. At this point, the Examiner should recognize that the claimed specific events are related to statuses of the finite-sate machine, as already commented above, and that the claimed service policies applied to the specific events result in state transitions in the specific instance identified by the assigned service session identifier.

However, Lev Ran's paragraph [0204], which has been specifically cited by the Examiner, discloses "Recurrence is a time property that can be applied to all directives. For example, discrete-time directive, such as for pre-positioning, can be activated every day at midnight. Similarly, a continuous-time directive, such as for a cache policy, can be activated every day between 9:00 a.m. and 5:00 p.m. Preferably, the recurrence granularity ranges from minutes (smallest) to years (largest)". This teaching discloses activation of recurrent directives, in particular for a cache policy, and nothing more than that. This teaching neither discloses nor suggests applying service policies to specific events related with statuses of a finite-state machine, and resulting in a state transition in the specific instance of the finite-state machine identified by the assigned service session identifier.

The Examiner has not substantiated why the skilled person aware of the activation of recurrent directives would have arrived to provide the claimed "activating service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier". Even if the Examiner, with a broad interpretation, might arrive to identify the "activation of recurrent directives" in Lev Ran with the "activating service policies applicable to said specific events" in claim 1, there is no motivation or suggestion for arriving to "the applied policies resulting in a state transition in the specific instance identified by the assigned service session identifier".

In addition, Lev Ran's paragraph [0459], which has been specifically cited by the Examiner in combination with Le Ran's paragraph [0204], discloses addressing and naming principles governing communications between RPC servers and RPC clients. In this respect, Lev Ran's paragraph [0450] discloses that "Remote services are activated by bidirectionally transferring remote procedure call (RPC) messages between a client application transport layer (RPC client) on one VFN gateway and a server application transport layer (RPC server) on a second remote VFN gateway. Following this definition, Lev Ran's paragraph [0459] teaches that, since an application transport layer may provide the same service on several remote servers, and each RPC server may offer more than one service, then an RPC request must identify the remote RPC

server to which it is addressed. More specifically, Lev Ran's paragraph [0459] cites using hostnames, or logical names, or path + port, or URN.

As such, Lev Ran's paragraph [0459] does not add any substantial contribution to the teaching in Lev Ran's paragraph [0204] which might be helpful for the skilled parson to arrive at the "activating service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier" as recited in claim 1. In view of at least the foregoing, Applicant respectfully submits that the independent claim 1 and the corresponding dependent claims 3-14 are patentable over Thomas, Lev Ran, or any combination thereof.

Applicant respectfully traverses the obviousness rejection of independent claim 15 in view Thomas, Lev Ran or any combination thereof. The independent claim 15 is as follows:

> 15. An Authorization Module suitable for use in a telecommunication system wherein a service network authenticates a user and authorizes the user for accessing a service offered by a service provider, the Authorization Module arranged for deciding whether a user is allowed to access a service and having:
> means for receiving a service authorization request from an Application Gateway Module; and
> means for returning to the Application Gateway Module a response on whether the user is granted access to the requested service;
> the Authorization Module comprising :
> means for generating a service session identifier intended to correlate those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;
> means for configuring a second finite-state machine with a number of statuses intended to identify specific events in service progression, the second finite-state machine usable by the Authorization Module to act over the Application Gateway Module to control the service progression;
> means for initiating a specific instance of the second finite-state machine, said specific instance being identified by said service session identifier; and
> means for determining service policies applicable to said specific events and resulting in a state transition in the specific instance identified by the assigned service session identifier.

The closest prior art Thomas discloses in paragraphs [0058]-[0059] an intermediary server and the Examiner interprets this entity as reading-on the claimed Authorization Module. Thomas's paragraph [0059] discloses client machines accessing

an intermediary server with requests for contents residing at private servers. The intermediary server, once the client machine is authenticated and authorized to get such contents, accesses the private server to obtain the requested contents and returns the contents to the requester client machine. Since, Thomas's intermediary server is interpreted as being both the Authorization Module and the Application Gateway Module in the present patent application, thus communications between these two modules are found to be implicitly disclosed in Thomas and thus not relevant distinguishing features to discuss hereinafter.

However, Thomas's paragraph [0072] discloses the intermediary server storing session identifiers, or cookies, for the clients or requesters. There is no specific teaching in this paragraph on whether a user may have more than one session identifier at a time. More specifically, Thomas's storing session identifiers for the clients does not teach the claimed "means for generating a service session identifier intended to correlate those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user". As already commented above with respect to claim 1, there is one service session identifier for each service delivery so that, where more than one service is delivered within a session, corresponding more than one service session identifiers are assigned, whereas Thomas does not teach the service session identifier for each service delivery.

Further, the Examiner interprets the teaching in Thomas's paragraph [0286] as teaching the claimed "means for configuring a second finite-state machine with a number of statuses intended to identify specific events in service progression, the second finite-state machine usable by the Authorization Module to act over the Application Gateway Module to control the service progression". This same teaching has been also used to object the first finite-state machine in the Application Gateway Module in the independent claim 1. Consequently, the same rationale used above in respect of Thomas's paragraph [0286] to defend the corresponding distinguishing feature of claim 1 can be used here to defend the second finite-state machine usable by the Authorization Module in claim 15.

Likewise, the Examiner interprets Thomas's paragraph [0069] in combination with paragraph [0286] as reading-on the claimed "means for initiating a specific instance of the second finite-state machine, said specific instance being identified by said service session identifier". The handling of cookies as disclosed in Thomas's paragraph [0069] has been discussed above with respect to claim 1 and is also applicable here. Consequently, the same rationale used above with respect to Thomas's paragraphs [0069] and [0286] to defend the corresponding distinguishing feature of claim 1 can be used here to defend the specific instance of the second finite-state machine, and identified by the service session identifier include in the Authorization Module under the independent claim 15.

Still further, the Examiner considers the teaching in Lev Ran's paragraphs [0204] and [0459] to read on the claimed "means for determining service policies applicable to said specific events and resulting in the state transition in the specific instance identified by the assigned service session identifier". Consequently, the same rationale used above with respect to Lev Ran's paragraphs [0204] and [0459] to defend the corresponding distinguishing feature of claim 1 can be used here as well to defend the claimed "means for determining service policies applicable to said specific events and resulting in the state transition in the specific instance identified by the assigned service session identifier". In view of at least the foregoing, Applicant respectfully submits that the independent claim 15 and the corresponding dependent claims 16, 18-24 are patentable over Thomas, Lev Ran, or any combination thereof.

Applicant respectfully submits that the independent claim 25 is also patentable in view of Thomas, Lev Ran or any combination thereof. The independent claim 25 recites the same or similar distinguishing limitations that have been discussed above with respect to the independent claims 1 and 15. As such, the aforementioned remarks regarding the patentability of the independent claims 1 and 15 apply as well to the independent claim 25. Accordingly, Applicant respectfully requests the allowance of the independent claim 25 and the corresponding dependent claims 27-30.

Remarks regarding the new independent claim 31

Applicant respectfully submits that new independent claim 31 is patentable in view of Thomas, Lev Ran or any combination thereof. The independent claim 31 is as follows:

> 31. An Application Gateway Module suitable for use in a telecommunication system wherein a service network authenticates a user and authorizes the user for accessing a service offered by a service provider, the Application Gateway Module arranged for intercepting application messages between the user and the service and for identifying said user and said service, the Application Gateway Module comprising:
>
> means for obtaining an authorization decision on whether the user is allowed to access the service;
>
> means for assigning a service session identifier intended to identify those application messages exchanged between the user and the service and that belong to a same service delivery authorized for said user;
>
> means for configuring a first finite-state machine with a number of statuses intended to identify specific events in service delivery, the first finite state machine configured to control service progression from a null state, a service authorization state, an active service state, and a disconnect service state; and
>
> means for activating service policies applicable to said specific events and resulting in a state transition in the first finite-state machine, the activating means further comprising:
>
> > means for statically arming at least one of the service policies before arrival of a first message to invoke the service; and
> >
> > means for dynamically arming at least one of the service policies during the progression of the service.

The new independent claim 31 has been added to indicate that the claimed means for activating service policies further includes: (1) means for statically arming at least one of the service policies before arrival of a first message to invoke the service; and (2) means for dynamically arming at least one of the service policies during the progression of the service. These new limitations along with limitations that are similar to the ones discussed above with respect to claim 1 clearly distinguishes the present invention over Thomas, Lev Ran or any combination thereof. Thus, Applicant respectfully submits that the new independent claim 31 is patentable over Thomas, Lev Ran or any combination thereof.

CONCLUSION

In view of the foregoing remarks, Applicant believes all of the claims currently pending in the application to be in a condition for allowance. Therefore, Applicant respectfully requests that the Examiner withdraw the pending objections and rejections and issue a Notice of Allowance for pending claims 1, 2-16, 18-25 and 27-31.

The Commissioner is hereby authorized to charge any fees for this paper to Deposit Account No. 50-1379.

Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

/William J. Tucker/

By William J. Tucker
Registration No. 41,356

Date: June 25, 2010

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(214) 324-7280 or (972) 583-2608
william.tucker@ericsson.com